WHAT IS CLAIMED IS:

1. A modular arithmetic apparatus for performing an arithmetic operation of an integer on the basis of a residue number system (RNS), comprising:

an input unit configured to input data included in modulus p and to output an arithmetic result;

a plurality of operation units configured to perform residue operations in parallel to obtain the arithmetic result, each operation unit having a storage unit which stores at least a portion of a plurality of base parameter sets, each one of said base parameter sets containing a different number of base parameters; and

a selection unit for configured to select one base parameter set in the plurality of base parameter sets according to the modulus p input from said input unit.

2. The apparatus of claim 1, wherein said selection unit selects a minimum base parameter set from said base parameter sets, for which a product of base elements is larger than the modulus p.

3. A modular arithmetic apparatus for performing an arithmetic operation of an integer on the basis of a residue number system (RNS), comprising:

an input/output unit configured to input data included in modulus p;

a plurality of operation units, each operation unit having a storage unit which stores at least a portion of a plurality of base parameter sets, each one of said base parameter sets containing a different number of base parameters;

a selection unit configured to select one base parameter set in the plurality of base parameter sets according to the modulus p input from said input/output unit;.

said plurality of operation units configured to perform residue operations in parallel according to the selected one base parameter set and to obtain an arithmetic result; and

said input/output unit configured to output the arithmetic result.

4. The apparatus of to claim 3, wherein said selection unit selects a minimum base parameter set from said base parameter sets which indicate that values of a product of base elements is larger than the modulus p.

5. A modular arithmetic apparatus for performing an arithmetic operation of an integer on the basis of a residue number system (RNS), comprising:

an input/output unit configured to input data included in modulus p and to output an arithmetic result;

a storage unit configured to store at least a portion of a plurality of base parameter sets, each base parameter set including a set of base parameters indicating base elements, each one of said plurality of base parameter sets contains a different number of base parameters, and

a base selection unit configured to select one base parameter set in said storage unit according to the modulus p input from said input/output unit; and

a plurality of arithmetic units configured to perform operations in parallel according to the selected one base parameter set to obtain the arithmetic result.

6. The apparatus of claim 5, wherein said base selection unit selects a minimum base parameter set from said base parameter sets, for which a product of base elements is larger than the modulus p.

7. The apparatus of claim 5, wherein the numbers of the base parameters of each base parameter set in said storage unit are multiples of the number of the arithmetic units, respectively.

8. The apparatus of claim 7, wherein said base selection unit selects a minimum base parameter set from said base parameter sets, from which a product of base elements is larger than the modulus p.

9. The apparatus of claim 5, wherein the numbers of the base parameters of each base parameter set in said storage unit are multiples of {u - t, u - t + 1, - - -, u}, respectively, said u is a number of the arithmetic units and said t is a maximum integer of a number of unused ones of the arithmetic units (t=0 or 0<t<u).

10. A modular arithmetic apparatus for performing an arithmetic operation of an integer on the basis of a residue number system (RNS), comprising:

an input/output unit configured to input data included in modulus p and to output an arithmetic result;

storage means for storing at least a portion of a plurality of base parameter sets, each base parameter including set comprises a set of base parameters indicating base elements, each one of said plurality of base parameter sets contains a different number of base parameters, and

a base selection means for selecting one base parameter set in said storage means according to the modulus p input from said input/output unit; and

a plurality of arithmetic units configured to perform operations in parallel according to the selected one base parameter set to obtain the arithmetic result.

11. The apparatus of claim 10, wherein said base selection means selects a minimum base parameter set from said base parameter sets, from which a product of base elements is larger than the modulus p.

12. A modular arithmetic apparatus for performing an arithmetic operation of an integer on the basis of a residue number system (RNS), comprising:

an input/output unit configured to input data included in modulus p and to output an arithmetic result;

a plurality of storage units configured to store at least a portion of a plurality of base parameter sets, each base parameter set including a set of base parameters indicating base elements, each one of said plurality of base parameter sets contains a different number of base parameters and;

a base selection unit configured to select one base parameter set in said storage units according to the modulus p input from said input/output unit; and,

a plurality of arithmetic units configured to perform operations in parallel according to the selected one base parameter set to obtain the arithmetic result.

13. The apparatus of claim 12, wherein said base selection units selects a minimum base parameter set from said base parameter sets, from which a product of base elements is larger than the modulus p.

14. A modular arithmetic method of performing an arithmetic operation of an integer on the basis of a residue number system (RNS) by a plurality of operation units in parallel, each operation unit having a storage unit which stores at least a portion of a plurality of base parameter sets each one of said base parameter sets containing a different number of base parameters, the method comprising:

inputting data included in modulus p;

selecting one base parameter set in the plurality of base parameter sets according to the input modulus p;

performing residue operations in parallel to obtain an arithmetic result; and

outputting the obtained arithmetic result.

15. The method of claim 14, wherein said selecting includes selecting a minimum base parameter set from said base parameter sets, from which a product of base elements is larger than the modulus p.

16. A modular arithmetic method of performing an arithmetic operation of an integer on the basis of a residue number system (RNS) by a plurality of operation units in parallel, the method comprising:

storing at least a portion of a plurality of base parameter sets to a storage unit, each base parameter set including a set of base parameters indicating base elements, each one of said plurality of base parameter sets contains a different number of base parameters inputting data included in modulus p;

selecting one base parameter set in said storage unit according to the input modulus p;

performing operations in parallel by the plurality of operation units according to a set of base parameters indicating the selected one base parameter set and obtaining an arithmetic result; and

outputting the obtained arithmetic result.

17. The method of claim 16, wherein said selecting includes selecting a minimum base parameter set from said base parameter sets, for which a product of base elements is larger than the modulus p.

18. The method of claim 16, wherein the numbers of the base parameters of each base parameter set in said storage unit are multiples of the number of the operation units, respectively.

19. The method of claim 18, wherein said selecting step selects a minimum base from said base parameter sets, for which a product of base elements is larger than the modulus p.

20. The method of claim 16, wherein the numbers of the base parameters of each base parameter set in said storage unit are multiples of {u - t, u - t + 1, ..., u}, respectively, said u is a number of the arithmetic units and said t is a maximum integer of a number of unused ones of the arithmetic units (t=0 or 0<t<u).